decide whether the requested information may be declassified, see § 60.7 and § 60.9.

(1) Unless withholding is otherwise warranted under applicable law, any information which may be declassified shall normally be forwarded to the requester within sixty (60) days after receipt of a proper request. If additional time is needed to locate or review the requested information, the Chief, Administrative Services Division will notify the requester accordingly. Except in unusual circumstances, a decision will be made within one year of receipt of the request.

(2) When information cannot be declassified in its entirety, a reasonable effort will be made, consistent with other applicable law, to release those portions of the requested information that constitute a coherent segment.

(3) Upon the denial or a partial denial of a request, the Chief, Administrative Services Division shall reply to the requester and provide a brief statement of the reasons for the denial, a notice of the right to appeal the decision to the Director, Office of Executive Administration and a notice that the appeal must be in writing and must be received by the Commission within sixty (60) days of receipt of the decision letter by the requester. Appeals should be addressed to: Director, Office of Executive Administration, Panama Canal Commission, Unit 2300, APO AA 34011–2300 (or Panama Canal Commission, Balboa Heights, Republic of Panama).

(e) Within thirty (30) days after its receipt of a proper appeal against an initial decision not to declassify information, the Director, Office of Executive Administration shall make and dispatch the decision whether the information should be declassified. If the Director, Office of Executive Administration is the original classification authority of the information under appeal, the Deputy Administrator shall determine whether the information may be declassified. The Director, Office of Executive Administration shall, after the decision, promptly make available to the requester any information that is declassified and which is otherwise releasable. If continued classification of the requested information is necessary, the requester shall be notified of that decision and the reasons therefor. If requested, the appeal determination shall also be communicated to any referring agency.

(f) The classification reviews made in response to requests and appeals under this section are in addition to the systematic review of classified information prescribed by Executive Order 12356 and 32 CFR part 2001.

(g) Requests for access to classified material submitted under the Freedom of Information Act or the Privacy Act of 1974 (5 U.S.C. 552 and 552a) shall be processed in accordance with parts 9 and 10 of 35 CFR, and shall be subject to the same review criteria for declassification as requests submitted under paragraphs (a) through (d) of this section. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order, the Commission shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under Executive Order 12356 or 32 CFR part 2001.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991; 59 FR 26123, May 19, 1994]

§ 60.13 Custody and storage.

(a) Classified information shall be protected in accordance with applicable National Security Council directives or directives promulgated by the Information Security Oversight Office and approved by the National Security Council.

(b) Each bureau director and chief of an independent unit (or classified security control officer as designated by the Director, Office of Executive Administration) shall be responsible for assuring that all classified information within that official's organization is used, processed, stored, and transmitted only under conditions which will provide adequate protection and prevent access by, or dissemination to, unauthorized persons. Containers, vaults, alarm systems, and associated security devices procured after the effective date of this part for the storage and protection of classified information

shall be in conformance with the standards and specifications published by the General Services Administration and, to the maximum extent practicable, be of the type designated on its Federal Supply Schedule.

(c)(1) Top secret information shall be stored in a GSA-approved security container with an approved built-in, three-position, dial-type combination lock; in a vault protected by an alarm system and response force; or in other storage facility that meets the standards for top secret established under the provisions of paragraph (b) of this section.

(2) Secret and confidential information shall be stored in a manner and under the conditions prescribed for top secret information, or in a container, vault, or alarmed area that meets the standards for secret or confidential information established pursuant to the provisions of paragraph (c)(1) of this section, and/or paragraph (c)(3) of this section.

(3) Secret and confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type, changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a three-position, changeable combination padlock approved by GSA for the purpose. The Director, Office of Executive Administration shall prescribe any necessary supplementary controls for storage of secret information in cabinets equipped with a steel lock bar.

(d) Each bureau director and chief of an independent unit (or classified security control officer) is responsible for assuring that all personnel within that official's organization, having access to classified information, have a security clearance issued by the Director, Office of Executive Administration, see § 60.14 and § 60.16.

(e)(1) Combinations of all repositories containing classified information shall be changed at least annually and forwarded in double-sealed envelopes to the Office of Executive Administration. The double-sealed envelopes shall be classified no lower than the highest category of information contained in the repositories. Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever the equipment is taken out of service, and at least once every year. Knowledge of combinations protecting classified information shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information to be stored in the security equipment concerned. Bureau directors and heads of independent units (or classified security control officers) shall ensure that combinations of dial-type locks shall be changed whenever there is reason to suspect possible compromise of the current combination.

(2) When security equipment having a built-in combination lock is taken out of service, the lock shall be reset to the standard combination 50–25–50. Combination padlocks shall be reset to the standard combination 10–20–30.

(3) The Commission shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected. Under no circumstances may keys be removed from the premises. They shall be stored in a secure container.

(f) Custodians of classified matter are responsible for registering with the Office of Executive Administration the names of all persons having knowledge of combinations to repositories containing classified information.

(1) Persons entrusted with classified information shall be responsible for providing protection and accountability for such information at all times and for locking classified information in approved security equipment whenever it is not in use or under the direct supervision of authorized persons. Custodians shall follow procedures which will ensure that unauthorized persons do not gain access to classified information.

(2) Individuals charged with the custody of classified information shall

conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. The Director, Office of Executive Administration shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by agency regulations are in effect at all times.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991]

§ 60.14 Security investigations; training and orientation of employees.

(a) Requests for security clearances, including changes in the level of clearances, will be forwarded to the Office of Personnel Administration for background investigations and security checks. The Deputy Personnel Director shall ensure that all necessary investigations are completed, and will provide a recommendation on the issuance of a security clearance to the Office of Executive Administration. The Director, Office of Executive Administration, in consideration of all available information, will determine if a security clearance may be issued, or if the level may be changed, and establish the expiration date of the clearance.

(b) The Director, Office of Executive Administration is also responsible for establishing and maintaining a training and orientation program for employees concerned with classified information or material.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59884, Nov. 26, 1991]

§ 60.15 Debriefing upon termination of employment.

(a) Bureau directors and heads of independent units (or classified security control officers as designated by the Director, Office of Executive Administration) shall be responsible for notifying the Office of Executive Administration whenever it is necessary that an employee be briefed or debriefed. Such notification should be in writing and be at least sixty (60) days, or as long as possible, in advance.

(b) Bureau directors and heads of independent units (or classified security control officers) shall ensure that debriefings are accomplished for any employee whose employment is terminated, or scheduled to be terminated, or when a temporary separation from employment (not to include leave) for sixty (60) days or more has occurred or is scheduled, whenever the employee has had access to classified information within the last twelve calendar months of his employment.

[56 FR 59884, Nov. 26, 1991]

§ 60.16 Responsibility of individual employees.

(a) The responsibility for the safeguarding of classified information shall rest on each individual employee having possession or knowledge of it, regardless of how such information or knowledge was obtained. In addition, each individual employee is directly responsible for acquiring familiarity with and complying with these and subsequently published security regulations.

(b) Any officer or employee, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by Executive Order 12356 or under this part, is subject to prompt and stringent administrative action, and, where a violation of criminal statute may be involved, is subject to prosecution under applicable law.

§ 60.17 Loss or compromise; destruction of nonrecord classified information.

(a) Any person who has knowledge of the loss or possible compromise of classified information in the custody of the Commission shall immediately report the circumstances to the Office of Executive Administration. The Director, Office of Executive Administration shall initiate an inquiry to:

(1) determine cause,

(2) place responsibility, and

(3) take corrective measures and appropriate administrative, disciplinary, or legal action. If it is determined that classified information has been compromised, the agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise.